UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,770	12/22/2000	Ron J. Vandergeest	10500.00.8171	4395

23418 7590 08/20/2008

VEDDER PRICE P.C.
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/747,770	VANDERGEEST ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date. _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12 June 2008 has been entered.

Response to Amendment

2. Applicant's amendment filed 12 June 2008 amends claims 6-10, 12-15, 17-21, and 23-31. Claims 1-5 have been cancelled. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant argues, "Since the web server is alleged to be the claimed first unit and since the session manager is in the same device as the web server, there is no authentication unit in Shi that receives from a different unit, the user ID data." In response, Applicant's specification does not support the authentication unit is a hardware device. Nowhere in the remarks section has Applicant pointed to support for this allegation. Instead, Applicant merely states that the authentication unit is inherently hardware. Contrary to Applicant's allegations the specification actually discloses that the authentication unit is a part of a web server (Page 12, lines 4-5). Therefore, the teachings of Shi still meet the claimed limitations.

4. Applicant argues, "Shi discloses that the web server transmits a generated unique ID to the same client which requests services…the 'client' in Shi is the same client that sends user identification data…the definition of 'first unit' apparently used to reject these claims is the

'client' of Shi." This argument is not persuasive because the Examiner has explained numerous times that the web server of Shi is relied upon to meet the claimed "first unit." Therefore, Applicant's entire argument with respect to remaining claims 8 and 19 appear to be based on this misconception, and are not persuasive.

5. Applicant argues, "Applicant's again respectfully request a showing as to how the alleged motivation is relevant to the claimed subject matter and further request an identification as to what corresponds to the claimed destination unit other than the first unit in either the Shi reference or the McCann reference." In response, Applicant's argument is based on the above mentioned misconception. Shi discloses that the web server transmits a generated unique id to the same client which requests services (Col. 8, lines 61-63). Shi does not disclose what client information is maintained allowing the unique id to be transmitted to the same client which requested services. One of ordinary skill in the art would understand that this could be accomplished by obtaining and storing the IP address of the client. McCann discloses obtaining and storing the IP address of a client for the duration of a communication session with an IP network (Abstract), which meets the limitation of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the user identification data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the session manager associated with the web server of Shi to obtain and store the IP address of the client in association with the user id/unique id in order to provide reduced response time as taught by McCann (Col. 1, lines 61-63).

6. Applicant's arguments with respect to the rejections of Shi, in view of Rahman have been fully considered and are persuasive. The rejections of claims 10-16, 21-26 over Shi, in view of Rahman have been withdrawn.

Allowable Subject Matter

7. The indicated allowability of claims 27-31 is withdrawn in view of the newly discovered reference(s) to Schmitz. Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 10-16, 21-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Claims 10, 21, 27 require primary authentication information to be transmitted from a primary authentication information provider to an authentication device on a first wireless channel during the same session as a the transmission of an authentication code to a destination device over a second wireless channel, which renders the claim indefinite because it is unclear how the destination device is apart of the communication session that was established prior to the determination step that actually found the particular destination device that would receive the authentication code. For the purpose of examination the claim limitations will be treated as occurring during the same authentication session.

11. Claims not listed are rejected based upon their dependence on claims 10, 21, and 27.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 6, 7, 17, 18 are rejected under 35 U.S.C. 102(b) as being anticipated by Shi, U.S. Patent No. 5,875,296. Referring to claims 6, 17, Shi discloses a web server user authentication system with cookies wherein a user provides a user id and password to a web server (Col. 8, lines 32-34). The web server sends the user id and password to the session manager for authentication using the DCE security service (Col. 6, lines 27-47 & Col. 8, lines 35-47), which meets the limitation of sending, by a first device, user identification data to an authentication device. If user authentication is successful a unique id is created for the user (Col. 8, lines 55-58), which meets the limitation of an authentication code. A cookie that includes the unique id is sent to the user (Col. 8, lines 61-63), which meets the limitation of using, user identification data, sent by the first device to determine which destination device will receive an authentication code to be used to authenticate the user, and sending the authentication code to determine destination device based on the user identification data because the web server knows which user terminal to transmit the created unique id based upon the previous user id and password that was previously submitted. On subsequent requests for service from the user, the unique id within the cookie, is

used as a pointer to the user's credentials in a credential database accessed by the session manager (Col. 6, lines 38-43 & Col. 8, line 66 – Col. 9, line 8), which meets the limitation of returning the authentication code to the authentication device, and authenticating the user when the returned authentication code matches the sent authentication code.

Referring to claims 7, 18, Shi discloses that the unique id is session based (Col. 3, lines 8-12), which meets the limitation of the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination device in response to the generated authentication code.

14. Claims 6-7, 10-13, 15-19, 21-24, 26-27, 29, 31 are rejected under 35 U.S.C. 102(a) and/or 102(e) as being anticipated by Schmitz, U.S. Patent No. 6,078,908. Referring to claims 6, 10, 17, 21, 27, Schmitz discloses a method for authorizing in data transmission systems wherein a user utilizes a first wireless device to transmit user identification information along a first wireless transmission path to an authorization computer (Col. 1, lines 45-50 & Col. 2, lines 57-63), which meets the limitation of sending primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication device during a session. The authorization computer utilizes the user identification information to determine which other wireless device of the user to transmit a generated password over a different transmission path (Col. 3, lines 1-28), which meets the limitation of using the primary authentication information to determine which destination device will receive an authentication code as secondary authentication information via a wireless back channel to be used to authenticate the user wherein the wireless back channel is an alternate channel to the primary wireless channel, sending the authentication code on the wireless back channel to the destination

device based on the primary authentication information during the same session. The user then manually inputs the received password into their first wireless device for transmission to the authorization computer over the first transmission path (Col. 1, lines 55-57 & Col. 2, lines 12-14 & Col. 3, lines 29-33), which meets the limitation of returning the authentication code on the wireless primary channel to the authentication device during the same session. The authorization computer compares the password received from the user with the password sent, and allows release of data to the first wireless unit (Col. 1, lines 58-62 & Col. 3, lines 36-42), which meets the limitation of authenticating the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel. The authorization computer includes memory (Col. 3, lines 19-20), which meets the limitation of memory containing executable instructions that when executed by one or more processors associated with one or more devices. The authorization computer can store the information about the other wireless devices of the user, or the authorization computer can utilize a data store to retrieve this information (Col. 3, lines 19-28), which meets the limitation of an authenticator operative to use the primary authentication information to determine which destination device, other than the first device, will receive an authentication code as secondary authentication information via the wireless back channel.

Referring to claims 7, 11, 22, Schmitz discloses that the generated password is generated for single use (Col. 3, lines 43-45), which meets the limitation of the steps of generating and sending the authentication code on a per authentication session basis.

Referring to claims 8, 12, 16, 23, Schmitz discloses that the authorization computer utilizes the user identification information to determine which other wireless device of the user to

transmit a generated password over a different transmission path (Col. 3, lines 1-28), which meets the limitation of the step of maintaining per user destination device data including at least one destination device identifier per user and wherein the step of using the primary authentication information to determine which destination device will receive the authentication code includes sending the authentication code to the destination device based on the stored per user destination device identifier, validating the primary authentication information.

Referring to claims 13, 24, 29, Schmitz discloses that the user then manually inputs the received password into their first wireless device for transmission to the authorization computer over the first transmission path (Col. 1, lines 55-57 & Col. 2, lines 12-14 & Col. 3, lines 29-33), which meets the limitation of the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication device until receipt of the user input, the first device includes an interface to receive user input in response to the sending of the authentication code and wherein the first device waits to return the authentication code for the authenticator until receipt of the user input.

Referring to claims 15, 26, 31, Schmitz discloses that the second wireless device could be a pager that receives the password using SMS (Col. 2, lines 46-49 & Col. 3, lines 7-9), which meets the limitation of the step of sending the authentication code on the wireless back channel to the destination device using at least one of a short message session (SMS) channel, a paging channel.

Referring to claim 18, Schmitz discloses that the generated password is generated for single use (Col. 3, lines 43-45) by an authorization computer with memory (Col. 3, lines 19-20), which meets the limitation of memory containing instructions that when executed by one or more

processors, causes the one or more processors to generate the authentication code on a per authentication session basis and send the authentication code to the determined destination device in response to the generated authentication code.

Referring to claim 19, Schmitz discloses that the authorization computer, with memory (Col. 3, lines 19-20), utilizes the user identification information to determine which other wireless device of the user to transmit a generated password over a different transmission path (Col. 3, lines 1-28), which meets the limitation of maintaining per user destination device data including at least one destination device identifier per user and wherein the step of using the primary authentication information to determine which destination device will receive the authentication code includes sending the authentication code to the destination device based on the stored per user destination device identifier

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

17. Claims 8, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shi, U.S. Patent No. 5,875,296, in view of McCann, U.S. Patent No. 6,052,725. Referring to claims 3, 8, 19, Shi discloses that the web server transmits a generated unique id to the same client which requests services (Col. 8, lines 61-63). Shi does not disclose what client information is maintained allowing the unique id to be transmitted to the same client which requested services. One of ordinary skill in the art would understand that this could be accomplished by obtaining and storing the IP address of the client. McCann discloses obtaining and storing the IP address of a client for the duration of a communication session with an IP network (Abstract), which meets the limitation of maintaining per user destination device data including at least one destination device identifier per user and wherein the step of using the user identification data to determine which destination device will receive the authentication code includes sending the authentication code to the determined destination device based on the stored per user destination device identifier. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the session manager associated with the web server of Shi to obtain and store the IP address of the client in association with the user id/unique id in order to provide reduced response time as taught by McCann (Col. 1, lines 61-63).

18. Claims 9, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shi, U.S. Patent No. 5,875,296, in view of Schneier, Applied Cryptography. Referring to claims 5, 9, 20, Shi does not disclose that the cookie is digitally signed prior to being authenticated by the session manager. It would have been obvious to one of ordinary skill in the art at the time the invention was made to digitally sign the cookie of Shi in order to verify the source of the cookie as a valid source as taught by Schneier (Pages 35-36).

19. Claims 9, 14, 20, 25, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schmitz, U.S. Patent No. 6,078,908, in view of Schneier. Referring to claims 9, 14, 20, 25, 30, Schmitz does not disclose that the first wireless device digitally signs the manually entered password prior to transmission to the authorization computer such that the authorization unit verifies the digital signature prior to password comparison. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the first wireless device to digitally sign the manually entered password prior to transmission to the authorization computer in order to provide the authorization computer a means to verify the source of the password as a valid source as taught by Schneier (Pages 35-36).

20. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schmitz, U.S. Patent No. 6,078,908. Referring to claim 28, Schmitz discloses that the authorization computer can store the information about the other wireless devices of the user, or the authorization computer can utilize a data store to retrieve this information (Col. 3, lines 19-28), which meets the limitation of the authenticator maintains per user destination device data including at least one destination device identifier per user. Schmitz also discloses that the password can be read from a data file (Col. 2, lines 65-67), but does not disclose where the data file is disclosed. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the data file that includes the passwords to be stored along with the second wireless device information in the data store coupled to the authorization computer (Col. 3, lines 23-28) because Schmitz discloses storage of information at the authorization computer or the data store in interchangeable embodiments that would have been implementable by those having

ordinary skill in the art in a predictable manner. Additionally, it is well known to store data externally to a computing system in order to free up storage space at the computing system.

Conclusion

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132